Attorney Docket No. 1466.1080

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Souichi OKADA et al.

Application No.: Group Art Unit:

Filed: Examiner:

For: PERSONAL IDENTIFICATION TERMINAL AND METHOD HAVING SELECTABLE IDENTIFICATION MEANS OR IDENTIFICATION LEVELS

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). JP 2002-345852

Filed: November 28, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Nov. 25, 2003 By: _____

H. J. Staas
Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１１月２８日

出 願 番 号
Application Number: 特願２００２－３４５８５２

[ST. 10/C]: [ＪＰ２００２－３４５８５２]

出 願 人
Applicant(s): 富士通株式会社

２００３年 ７月 ９日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号 出証特２００３－３０５５４３５

【書類名】　特許願
【整理番号】　0295575
【提出日】　平成14年11月28日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00
【発明の名称】　個人認証端末、個人認証方法及びコンピュータプログラム
【請求項の数】　10
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　岡田　壮一
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　長谷部　高行
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　蒲田　順
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　林　武彦
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100086933

【弁理士】

【氏名又は名称】　久保　幸雄

【電話番号】　06-6304-1590

【手数料の表示】

【予納台帳番号】　010995

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9704487

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　個人認証端末、個人認証方法及びコンピュータプログラム

【特許請求の範囲】

【請求項１】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末であって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定することを特徴とする個人認証端末。

【請求項２】

前記認証手段・レベル指定情報は、電子署名された情報のように、改竄検出可能な形式の情報であることを特徴とする

請求項１記載の個人認証端末。

【請求項３】

前記認証手段・レベル指定情報によって指定された認証手段又は認証レベルが存在しない場合は、あらかじめ定められた認証手段又は認証レベルを使用して個人認証を行うことを特徴とする

請求項１記載の個人認証端末。

【請求項４】

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする

請求項１記載の個人認証端末。

【請求項５】

前記改竄検出可能な形式は、秘密鍵を用いたネットワーク認証プロトコルによるものであることを特徴とする

請求項４記載の個人認証端末。

【請求項６】

認証手段又は認証レベルごとに異なる秘密鍵を使用することを特徴とする

請求項５記載の個人認証端末。

【請求項７】

生体情報による認証手段を使用した場合に、前記認証結果の情報に類似度であるスコアを付加することを特徴とする

請求項４記載の個人認証端末。

【請求項８】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末に対して、サーバーから認証要求と共に認証手段・レベル指定情報を送信し、

前記個人認証端末はサーバーから受信した前記認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定し、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする個人認証方法。

【請求項９】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムであって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とするコンピュータプログラム。

【請求項１０】

複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、前記コンピュータプログラムが

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステッ

プと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数の認証手段を備え、認証の目的、用途又はシステムのセキュリティレベルに応じて使用する認証手段や認証レベルを選択することができる個人認証端末、個人認証方法及びコンピュータプログラムに関する。

【０００２】

【従来の技術】

あらかじめ登録された本人であることをその人の持ち物（ＩＤカード等）、記憶（パスワード等）又は生体情報（指紋等）を用いて認証する個人認証技術は、入退室管理やパーソナルコンピュータのログイン管理等に使用されている。このような個人認証技術には、パスワードやＩＤカードを用いる比較的簡単なものから指紋、声紋、虹彩等を用いた高度なものまである。また、複数種類（マルチモーダル）の認証手段や認証レベルを備え、それらの組み合わせによってセキュリティの向上を図っているものもある。

【０００３】

例えば、特開２０００－１３７８４４号公報には、勤務時間帯や部屋状況に応じて認証手段（磁気カード、ＩＣカード、指紋等）を変える技術が開示されている。特開２０００－１４５２１９号公報には、部屋のセキュリティレベルに応じて生体情報による認証の精度（レベル）を設定する技術が開示されている。特開２０００－２１５１７２号公報には、セキュリティレベルに応じて認証手段（暗証番号、生体情報又はパスワード）を変える技術が開示されている。特開２０００－２１５２７９号公報には、決済金額に応じて認証手段（暗証番号又は指紋）を変える技術が開示されている。

【０００４】

上記のような個人認証装置をサーバーと接続された個人認証端末として使用する形態がある。サーバーに対してサービスの提供を希望するユーザは、個人認証端末を用いてＩＤ、暗証番号、生態情報等を入力し、その結果、正規ユーザであることが認証された後に所望のサービスを受けることができる。この場合、生体情報等の個人情報は個人認証端末側で管理され、サーバーから個人認証装置に対して個人認証の実行を要求し、認証結果が個人認証装置からサーバーに返される。

【０００５】

【発明が解決しようとする課題】

複数の認証手段や認証レベルを選択して使用できる個人認証端末において、ユーザが複数の認証手段や認証レベルの中から使用すべき認証手段や認証レベルを選択する必要があるとすれば、ユーザ操作の負担が大きく、使い勝手の悪いものとなる。また、サーバーからの指令により使用すべき認証手段や認証レベルが個人認証端末で指定される場合であっても、認証結果のみが個人認証端末からサーバーに返されるとすれば、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに改竄し、あるいは認証レベルを下げる改竄を行うような不正使用のおそれがある。

【０００６】

本発明は、上記のような課題に鑑み、サーバーからの認証要求に応じて個人認証を実行する個人認証端末において、悪意のあるユーザによる不正使用を防止して認証結果の信頼性を高めることを目的とする。

【０００７】

【課題を解決するための手段】

本発明による個人認証端末は、複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末であって、サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定することを特徴とする。

【０００８】

このような構成によれば、サーバーからの指令によって使用すべき認証手段や

認証レベルが個人認証端末に指定されるので、ユーザ操作の負担が軽くなり、使い勝手が良くなる。

【０００９】

好ましくは、前記認証手段・レベル指定情報は、電子署名された情報のように、改竄検出可能な形式の情報である。これにより、個人認証のセキュリティが高くなる。

【００１０】

また、前記認証手段・レベル指定情報によって指定された認証手段又は認証レベルが存在しない場合は、あらかじめ定められた（つまりデフォルトの）認証手段又は認証レベルを使用して個人認証を行うことが好ましい。これにより、サーバーからの認証手段又は認証レベルの指定が間違っている場合にも処理を停止することなく対応することができる。

【００１１】

更に、本発明による個人認証端末は、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返す。これにより、サーバーは、指定した認証手段又は認証レベルで個人認証が正しく行われたことを確認することができる。換言すると、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに改竄し、あるいは認証レベルを下げる改竄を行うような不正使用を排除することが可能になる。

【００１２】

上記の改竄検出可能な形式は、秘密鍵を用いたネットワーク認証プロトコルによるものであることが好ましい。この場合、認証手段又は認証レベルごとに異なる秘密鍵を使用することが更に好ましい。

【００１３】

また、本発明による個人認証端末は、生体情報（指紋、声紋、虹彩等）による認証手段を使用した場合に、類似度であるスコア又はそのハッシュ値を前記認証結果の情報に付加することが好ましい。合格（ＯＫ）又は不合格（ＮＧ）の認証結果だけでなく、スコア又はそのハッシュ値を付加することにより、サーバー側でのきめ細かな対応が可能になる。スコアをそのまま送ってもよいが、そのハッ

シュ値として送ることによりセキュリティが高くなる。

【００１４】

本発明による個人認証方法は、複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末に対して、サーバーから認証要求と共に認証手段・レベル指定情報を送信し、前記個人認証端末はサーバーから受信した認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定し、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする。

【００１５】

このような個人認証方法によれば、ユーザ操作の負担が軽くなり個人認証端末の使い勝手が良くなると共に、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに変えたり認証レベルを下げたりする改竄行為を排除することが可能になる。

【００１６】

本発明によるコンピュータプログラムは、複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムであって、サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とする。

【００１７】

このようなコンピュータプログラムを処理装置に実行させることにより、ユーザ操作の負担が軽くなり個人認証端末の使い勝手が良くなると共に、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに変えたり認証レベルを下げたりする改竄行為を排除することが可能になる。

【００１８】

このようなコンピュータプログラムは、例えばＣＤ－ＲＯＭのようなコンピュ

ータ読み取り可能な記憶媒体に記録された状態で供給され、記憶媒体からコンピュータにインストールされ実行される。あるいはネットワークに接続されたサーバー等の他のコンピュータからダウンロードしてインストールし、又は逐次実行することも可能である。

【００１９】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

図１は、本発明の実施形態に係る個人認証端末の構成例を示すブロック図である。この個人認証端末１は、複数種類の認証手段による認証を行うために、複数の（第１～第ｎの）認証情報入力部１１を備えている。認証情報入力部１１の具体的な構成としては、暗証番号やパスワードを入力するためのキーボード、生体情報（指紋、声紋、虹彩等）を入力するためのセンサー（センサーチップ、マイクロフォン、ＣＣＤカメラ等）のような既存のデバイスを使用することができる。また、個人認証端末１はセキュリティレベルに応じて複数の認証手段や認証レベルの中から１つの認証手段や認証レベルを選択するためのセレクタ１２及び認証手段・レベル設定部１３を備えている。

【００２０】

個人認証端末１は更に、ＣＰＵ（処理装置）１４、認証情報格納部１５及びプログラム格納部１６を備えている。プログラム格納部１６に格納されたプログラムにしたがってＣＰＵ１４が認証（照合）処理を実行する。この際、認証手段・レベル設定部１３で設定された認証手段と認証レベルで認証処理が行われる。認証情報格納部１５には、認証処理に必要な認証情報、すなわち暗証番号、パスワード、生体情報、ＰＫＩ（パブリック・キー・インフラストラクチュア）証明書、秘密鍵等が格納されている。

【００２１】

なお、認証処理用のプログラムは、例えばＣＤ－ＲＯＭのような記憶媒体２０に記憶された状態で供給され、読取装置２１を介してプログラム格納部（例えば固定ディスク装置）１６にインストールされる。後述する通信インターフェイス部１７を介してネットワークに接続された他のコンピュータ（サーバー）から認

証処理用のプログラムをダウンロードしてプログラム格納部１６にインストールしてもよい。

【００２２】

また、個人認証端末１は、通信インターフェイス部１７と暗号化・署名処理部１８を備えている。通信インターフェイス部１７の働きにより、個人認証端末１は各種サービスを提供するサーバー２にネットワークを介して接続することができる。サーバー２は、例えばパーソナルコンピュータのような端末装置を用いてサービスの提供を求めてきたユーザがあらかじめ登録された正規ユーザであることの認証を行うために、そのユーザがアクセス可能な（例えば端末装置の近くに設置された）個人認証端末１に認証要求を送信する。

【００２３】

この際、認証要求と共に、認証に使用すべき認証手段や認証レベルを指定するための認証手段・レベル指定情報がサーバー２から個人認証端末１に送信される。もちろん、認証手段・レベル指定情報が認証要求に含まれる形式で送信されてもよい。この場合、上述のセレクタ１２及び認証手段・レベル設定部１３は、サーバー２から受信した認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定する。

【００２４】

また、個人認証端末１は、認証結果と共に、実際に認証に使用した認証手段及び認証レベルを特定する使用手段・レベル情報をサーバー２に返す（送信する）。これは、サーバー２から個人認証端末１に送信した認証手段・レベル指定情報で指定された認証手段及び認証レベルで認証が正しく行われたことをサーバー２が確認できるようにするためである。この使用手段・レベル情報は、改竄されないように（もし改竄されれば検出できるように）、暗号化・署名処理部１８によって電子署名が付された後にサーバー２へ送信される。必要な場合は、暗号化・署名処理部１８によって暗号化も行われる。

【００２５】

また、個人認証端末１において、認証情報として生体情報が用いられた場合は、照合処理の中で計算されるスコア（類似度）又はスコアのハッシュ値（ハッシ

ュ関数で計算された値）が認証結果と共に個人認証端末１からサーバー２に送信される。スコアをそのまま送るのではなくハッシュ値として送ることにより、暗号化と同様にセキュリティが高まる。

【００２６】

更に、個人認証端末１は次認証手段判断部１９を備えている。ある生体情報による認証手段を用いて認証を行ったときのスコアがＣＰＵ１４から次認証手段判断部１９に通知されると、次認証手段判断部１９はそのスコアに基づいて次に使用すべき生体情報による認証手段を判断してＣＰＵ１４に通知する。例えば、声紋による認証手段を用いて認証を行った結果、ある程度の類似度（スコア）が得られたもののＯＫ（合格）レベルに達しなかった場合に、次認証手段判断部１９が次に使用すべき生体情報による認証手段として指紋による認証手段をＣＰＵ１４に通知する。

【００２７】

但し、次認証手段判断部１９が働くのは、サーバー２から送信された認証手段・レベル指定情報で複数の認証手段が指定された場合である。１つだけの認証手段が指定された場合は次認証手段判断部１９が働く余地はない。

【００２８】

また、ある生体情報による認証手段を用いて認証を行ったときのスコアがあらかじめ定めた最低レベルより低い場合に、ＣＰＵ１４は次の認証処理に進むことなく処理を停止する。また、ある生体情報による認証手段を使用して認証を行ったときの類似度であるスコアが完全一致を示している場合は認証結果を不合格（ＮＧ）とする。生体情報による認証では、生体情報の経年変化や外部環境の相違に起因して、認証情報格納部１５に格納されている照合用の生体情報と入力された生体情報とが完全一致することは極めて稀である。そこで、スコアが完全一致を示している場合は、悪意のある使用者が何らかの方法で入手した照合用の生体情報を入力した可能性が高いので、上記のように認証結果を不合格（ＮＧ）とする。

【００２９】

図２は、生体情報による認証手段を用いて認証を行う場合の照合処理の例を示

すフローチャートである。先ずステップ＃１０１でスコアＳを計算する。つまり、図１の認証情報入力部１１から入力された生体情報を認証情報格納部１５から読み出した照合用の生体情報と比較して、類似度であるスコアＳを計算する。続くステップ＃１０２で、スコアＳをあらかじめ定めた最低レベルＸｍｉｎと比較する。スコアＳが最低レベルＸｍｉｎより低い場合は、ステップ＃１０７へ移行して処理を停止する。

【００３０】

スコアＳが最低レベルＸｍｉｎより高い場合は、次のステップ＃１０３でスコアＳが１００であるか否かをチェックする。この例では、スコアＳは０～１００の値をとり得る。そして、スコアＳが１００である場合は、照合用の生体情報と入力された生体情報とが完全一致することを示しているので、ステップ＃１０６に移行して照合結果が不合格（ＮＧ）であると判定する。

【００３１】

スコアＳが１００でない場合は、次のステップ＃１０４でスコアＳを合否判定値Ｘｒと比較する。スコアＳが合否判定値Ｘｒより低い場合はステップ＃１０６に移行して照合結果が不合格（ＮＧ）であると判定し、スコアＳが合否判定値Ｘｒ以上である場合はステップ＃１０５へ移行して照合結果が合格（ＯＫ）であると判定する。なお、スコアＳの最低レベルＸｍｉｎ及び合否判定値Ｘｒはセキュリティレベルに応じてあらかじめ設定されている。

【００３２】

図３は、個人認証端末１をＩＣカード１ａとＩＣカードリーダライタ１ｂとの組み合わせによって構成した例を示すブロック図である。この構成例では、ＩＣカード１ａの側にＣＰＵ１４、認証情報格納部１５、プログラム格納部１６及び次認証手段判断部１９が備えられ、ＩＣカードリーダライタ１ｂの側に認証情報入力部１１、セレクタ１２、認証手段・レベル設定部１３、通信インターフェイス部１７及び暗号化・署名処理部１８が備えられている。また、ＩＣカード１とＩＣカードリーダライタ１ｂとの間の通信をおこなうためのインターフェイス２３，２４がそれぞれに備えられている。

【００３３】

図４は、一定の条件を満たした場合にサーバー側で認証不合格と判断するシステム構成の例を示すブロック図である。この構成例のサーバー２は、個人認証端末１から通信インターフェイス部２７を介して受信した認証結果の情報に付加されたスコアのログを格納するスコアログ格納部２５と、スコアログ格納部２５から読み出したスコア又はそのハッシュ値のログに基づいて、同じスコアが複数回（例えば５回）連続した場合は個人認証端末から受信した認証結果にかかわらず認証不合格（ＮＧ）と判定する処理部２６とを備えている。生体情報による認証では、生体情報の経年変化や外部環境の変化に起因して、認証の類似度であるスコアが毎回同じであることは極めて稀である。同じスコアが複数回連続した場合は、悪意のあるユーザによって人工的に作られた生体情報が毎回入力された可能性が高い。そこで、このサーバー２では、そのような場合は認証不合格（ＮＧ）と判定し、サービスの提供を行わない。

【００３４】

図５は、個人認証端末から取得した情報に基づいてサーバーが認証手段・レベル指定情報を変更するシステム構成の例を示すブロック図である。この構成例では、個人認証端末１にＲＴＣ・ＧＰＳ部３０が備えられている。ＲＴＣ（リアルタイムクロック）は、現在の日付及び時刻の情報を生成し出力する。ＧＰＳ（グローバルポジショニングシステム）は、個人認証端末１の位置情報を生成して出力する。

【００３５】

サーバー２から個人認証端末１への認証要求及び認証手段・レベル指定情報の送信に先立って、ＲＴＣ・ＧＰＳ部３０から出力された現在の日付及び時刻の情報と位置情報を含む認証端末情報が個人認証端末１からサーバー２に送信される。サーバー２の処理部２６は、受信した認証端末情報にしたがって、個人認証端末１に送信する認証手段・レベル指定情報を変更する。これにより、サーバー２がサービスの提供を開始する際に、又は認証を行うたびに、認証手段及びレベルが個人認証端末１に設定される。

【００３６】

なお、現在の日付及び時刻の情報と位置情報の両方を認証端末情報に含める必

要は必ずしも無く、少なくともいずれか一方が含まれておればよい。また、個人認証端末１の装置ＩＤを認証端末情報に含めてもよい。

【００３７】

図６は、チャレンジ＆レスポンスによる認証手段又は認証レベルの確認方法の例を示す図である。先ず、サーバー２から個人認証端末１に認証手段・レベル指定情報が送信される（ステップ＃２０１）。認証手段・レベル指定情報を受信した個人認証端末１は、認証手段・レベル指定情報にしたがって使用する認証手段又は認証レベルを設定し、生体情報を入力して照合処理を行う（ステップ＃２０２）。

【００３８】

照合処理が完了するとチャレンジコード要求（処理完了通知）が個人認証端末１からサーバー２に送信される（ステップ＃２０３）。チャレンジコード要求を受信したサーバー２は、乱数をチャレンジコードとして個人認証端末１に送信する（ステップ＃２０４）。チャレンジコードを受信した個人認証端末１は、乱数、使用手段・レベル情報、スコア又はそのハッシュ値等を結合して得られるレスポンスコードをサーバー２に送信する（返す）（ステップ＃２０５）。この際、改竄を検出するためのＰＫＩ署名を付して送信する。レスポンスコードを受信したサーバー２は、指定した認証手段及び認証レベルで認証が行われたことをレスポンスコードから確認することができる。

【００３９】

図７は、認証結果が合格である場合に、ユーザによる秘密鍵の利用回数を制限するための構成例を示す図である。ステップ＃３０１でユーザ（個人認証端末１の側）からサーバー２にサービス要求が送信されると、サーバー２は認証手段・レベル指定情報と共に秘密鍵の利用回数を指定するための利用回数設定情報を個人認証端末１に送信する（ステップ＃３０２）。認証手段・レベル指定情報と利用回数設定情報を受信した個人認証端末１は、認証手段・レベル指定情報にしたがって使用する認証手段又は認証レベルを設定し、生体情報を入力して照合処理を行う（ステップ＃３０３）。照合処理が完了するとチャレンジコード要求（処理完了通知）が個人認証端末１からサーバー２に送信される（ステップ＃３０４

）。

【００４０】

また、認証結果がＯＫ（合格）のときに、個人認証端末１は秘密鍵の利用回数を利用回数カウンタに設定し、秘密鍵が使用されるたびに利用回数カウンタをデクリメントする利用回数管理処理を実行する（ステップ＃３０５）。利用回数カウンタがゼロになれば、秘密鍵の利用ができなくなる。

【００４１】

チャレンジコード要求を受信したサーバー２は、乱数からなるチャレンジコードを生成し、個人認証端末１に送信する（ステップ＃３０６）。チャレンジコードを受信した個人認証端末１は、乱数、使用手段・レベル情報、スコア又はそのハッシュ値、そして利用回数情報を結合して得られるレスポンスコードをサーバー２に送信する（返す）（ステップ＃３０７）。この際、改竄を検出するためのＰＫＩ署名がレスポンスコードに付される。レスポンスコードを受信したサーバー２は、指定した認証手段及び認証レベルで認証が行われたこと、そして設定した秘密鍵の利用回数が改竄されていないことをレスポンスコードから確認することができる。

【００４２】

以上、本発明の実施形態をいくつかの実施例と共に説明したが、本発明は上記実施形態に限定されず種々の形態で実施することが可能である。

（付記１）複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末であって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定することを特徴とする個人認証端末。

【００４３】

（付記２）前記認証手段・レベル指定情報は、電子署名された情報のように、改竄検出可能な形式の情報であることを特徴とする付記１記載の個人認証端末。

（付記３）前記認証手段・レベル指定情報によって指定された認証手段又は認証レベルが存在しない場合は、あらかじめ定められた認証手段又は認証レベルを

使用して個人認証を行うことを特徴とする付記１記載の個人認証端末。

【００４４】

（付記４）実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする付記１記載の個人認証端末。

【００４５】

（付記５）前記改竄検出可能な形式は、秘密鍵を用いたネットワーク認証プロトコルによるものであることを特徴とする付記４記載の個人認証端末。

（付記６）認証手段又は認証レベルごとに異なる秘密鍵を使用することを特徴とする付記５記載の個人認証端末。

【００４６】

（付記７）前記認証結果の情報に前記使用手段・レベル情報を付加した情報を暗号化し、又は電子署名を付してサーバーに返すことを特徴とする付記４記載の個人認証端末。

【００４７】

（付記８）生体情報による認証手段を使用した場合に、類似度であるスコア又はそのハッシュ値を前記認証結果の情報に付加することを特徴とする付記４記載の個人認証端末。

【００４８】

（付記９）生体情報による認証手段を使用して認証を行ったときの類似度であるスコアに応じて、次に使用すべき生体情報による認証手段の決定を行うための次認証手段判断部を更に備えていることを特徴とする付記４記載の個人認証端末。

【００４９】

（付記１０）生体情報による認証手段を使用して認証を行ったときの類似度であるスコアがあらかじめ定めた最低レベルより低い場合は次の認証処理に進むことなく処理を停止することを特徴とする付記９記載の個人認証端末。

【００５０】

（付記１１）生体情報による認証手段を使用して認証を行ったときの類似度で

あるスコアが完全一致を示している場合は認証結果を不合格とすることを特徴とする付記４記載の個人認証端末。

【００５１】

（付記１２）前記個人認証端末が、ＩＣカードとＩＣカードリーダライタとの組み合わせによって構成されていることを特徴とする付記１記載の個人認証端末。

【００５２】

（付記１３）付記８記載の個人認証端末から受信した認証結果の情報に付加されたスコア又はそのハッシュ値のログを格納するスコアログ格納部と、スコアログ格納部から読み出したスコア又はそのハッシュ値のログに基づいて、同じスコアが複数回連続した場合は個人認証端末から受信した認証結果にかかわらず認証不合格と判断する処理部とを備えていることを特徴とするサーバー。

【００５３】

（付記１４）複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末に対して、サーバーから認証要求と共に認証手段・レベル指定情報を送信し、

前記個人認証端末はサーバーから受信した認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定し、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すことを特徴とする個人認証方法。

【００５４】

（付記１５）前記サーバーから前記個人認証端末への認証要求及び認証手段・レベル指定情報の送信に先立って、前記個人認証端末から位置又は現在時刻の情報を含む認証端末情報をサーバーに送信し、サーバーの処理部は、個人認証端末から受信した認証端末情報にしたがって、個人認証端末に送信する認証手段・レベル指定情報を変更することを特徴とする付記１４記載の個人認証方法。

【００５５】

（付記１６）前記認証要求及び認証手段・レベル指定情報と共に、秘密鍵の利用回数指定情報をサーバーから前記個人認証端末へ送信し、認証結果が合格であ

る場合に、ユーザによる秘密鍵の利用回数を制限することを特徴とする付記１４記載の個人認証方法。

【００５６】

（付記１７）複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムであって、

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とするコンピュータプログラム。

【００５７】

（付記１８）複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末の処理装置に実行させるコンピュータプログラムが記憶されたコンピュータ読み取り可能な記憶媒体であって、前記コンピュータプログラムが

サーバーから認証要求を受信するたびに、サーバーから受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定するステップと、

実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返すステップとを備えていることを特徴とする記憶媒体。

【００５８】

【発明の効果】

以上に説明したように、本発明の個人認証端末、個人認証方法及びコンピュータプログラムによれば、サーバーからの指令によって使用すべき認証手段や認証レベルが個人認証端末に指定されるので、ユーザ操作の負担が軽くなり、個人認証端末の使い勝手が良くなる。また、サーバーは指定した認証手段又は認証レベ

ルで個人認証が正しく行われたことを確認することができるので、悪意のあるユーザが個人認証端末側で認証手段を都合の良いものに改竄し、あるいは認証レベルを下げる改竄を行うような不正使用を排除することが可能になる。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る個人認証端末の構成例を示すブロック図である。

【図２】

生体情報による認証手段を用いて認証を行う場合の照合処理の例を示すフローチャートである。

【図３】

個人認証端末をＩＣカードとＩＣカードリーダライタとの組み合わせによって構成した例を示すブロック図である。

【図４】

一定の条件を満たした場合にサーバー側で認証不合格と判断するシステム構成の例を示すブロック図である。

【図５】

個人認証端末から取得した情報に基づいてサーバーが認証手段・レベル指定情報を変更するシステム構成の例を示すブロック図である。

【図６】

チャレンジ＆レスポンスによる認証方法又は認証レベルの確認方法の例を示す図である。

【図７】

認証結果が合格である場合に、ユーザによる秘密鍵の利用回数を制限するための構成例を示す図である。

【符号の説明】

１　個人認証端末

２　サーバー

１１　認証情報入力部

１２　セレクタ

１３　認証手段・レベル設定部

１４　ＣＰＵ（処理装置）

１５　認証情報格納部

１６　プログラム格納部

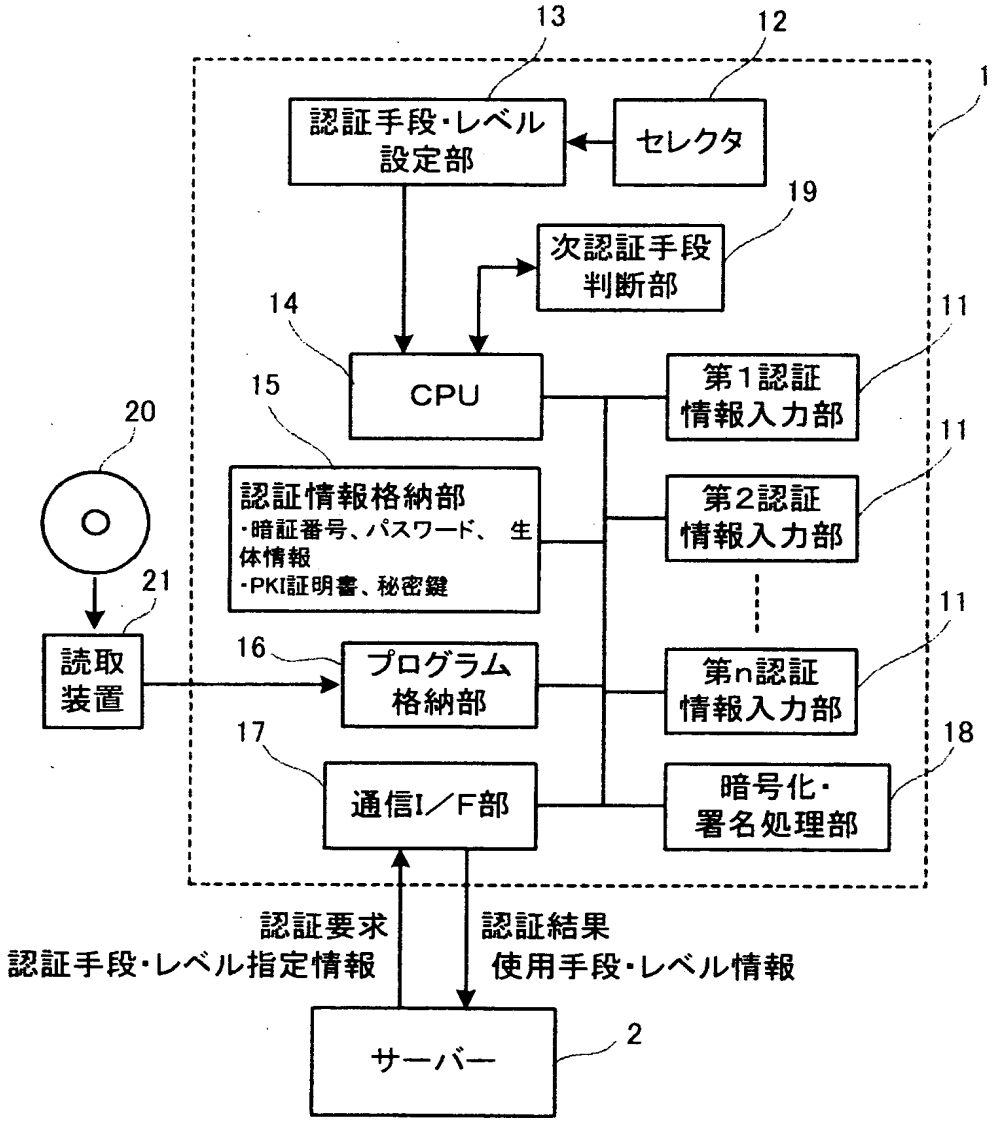
１８　暗号化・署名処理部

１９　次認証手段判断部

【書類名】　図面

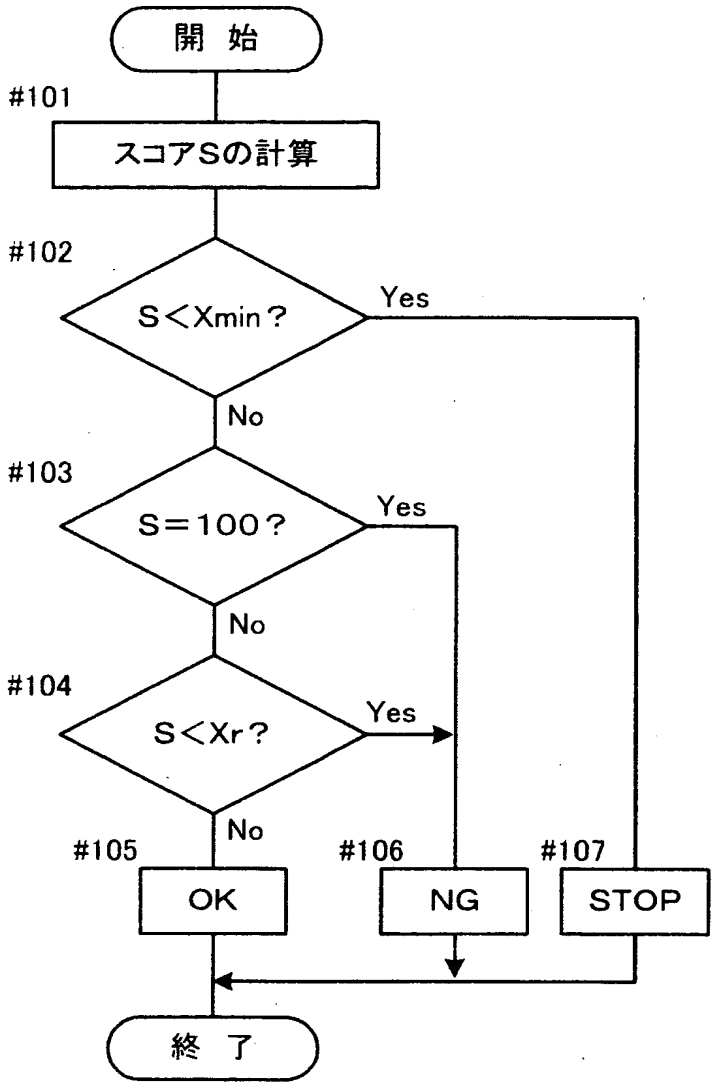
【図１】

本発明の実施形態に係る個人認証端末の構成例を示すブロック図



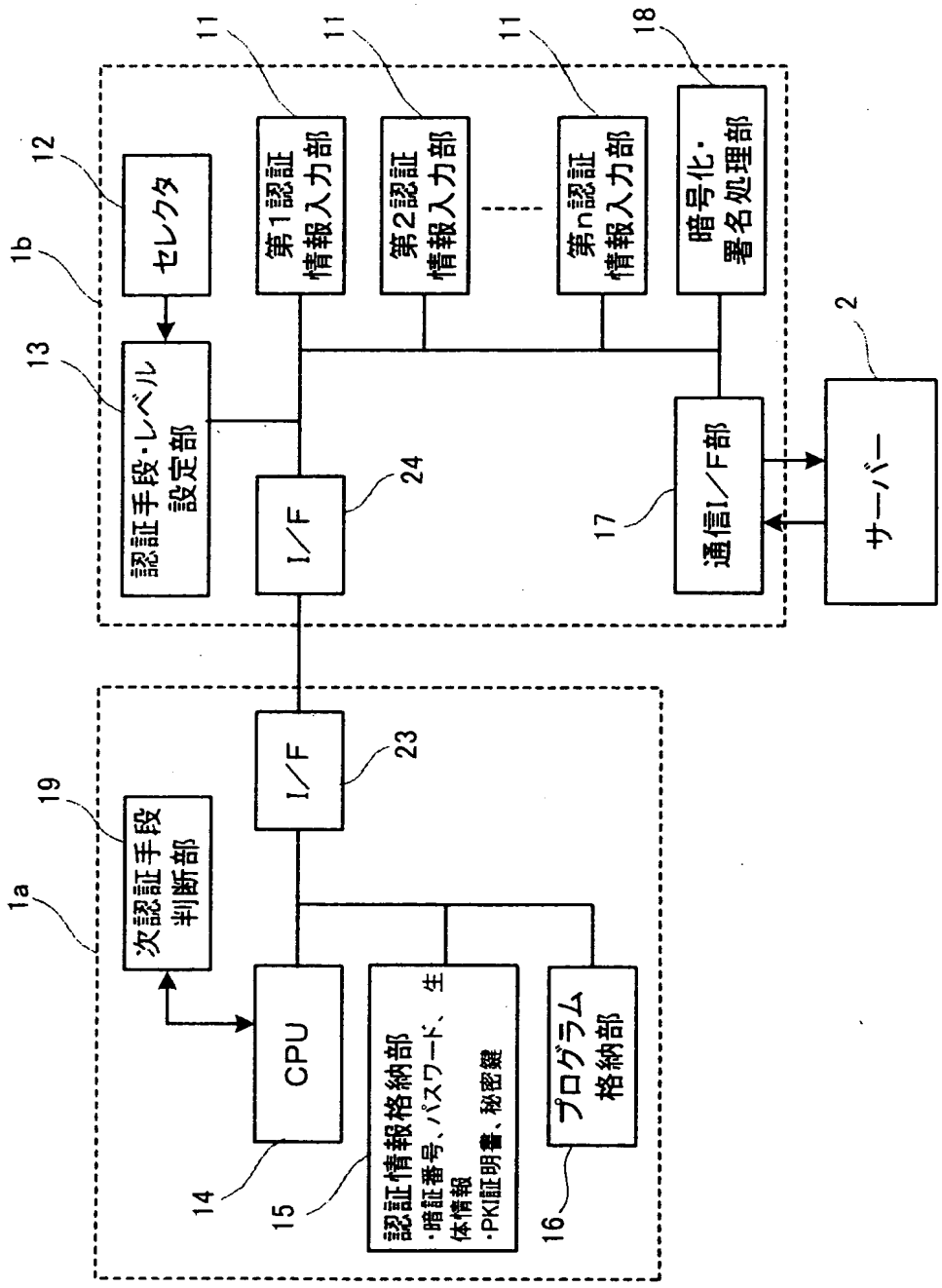
【図２】

生体情報による認証手段を用いて認証を行う場合の
照合処理の例を示すフローチャート



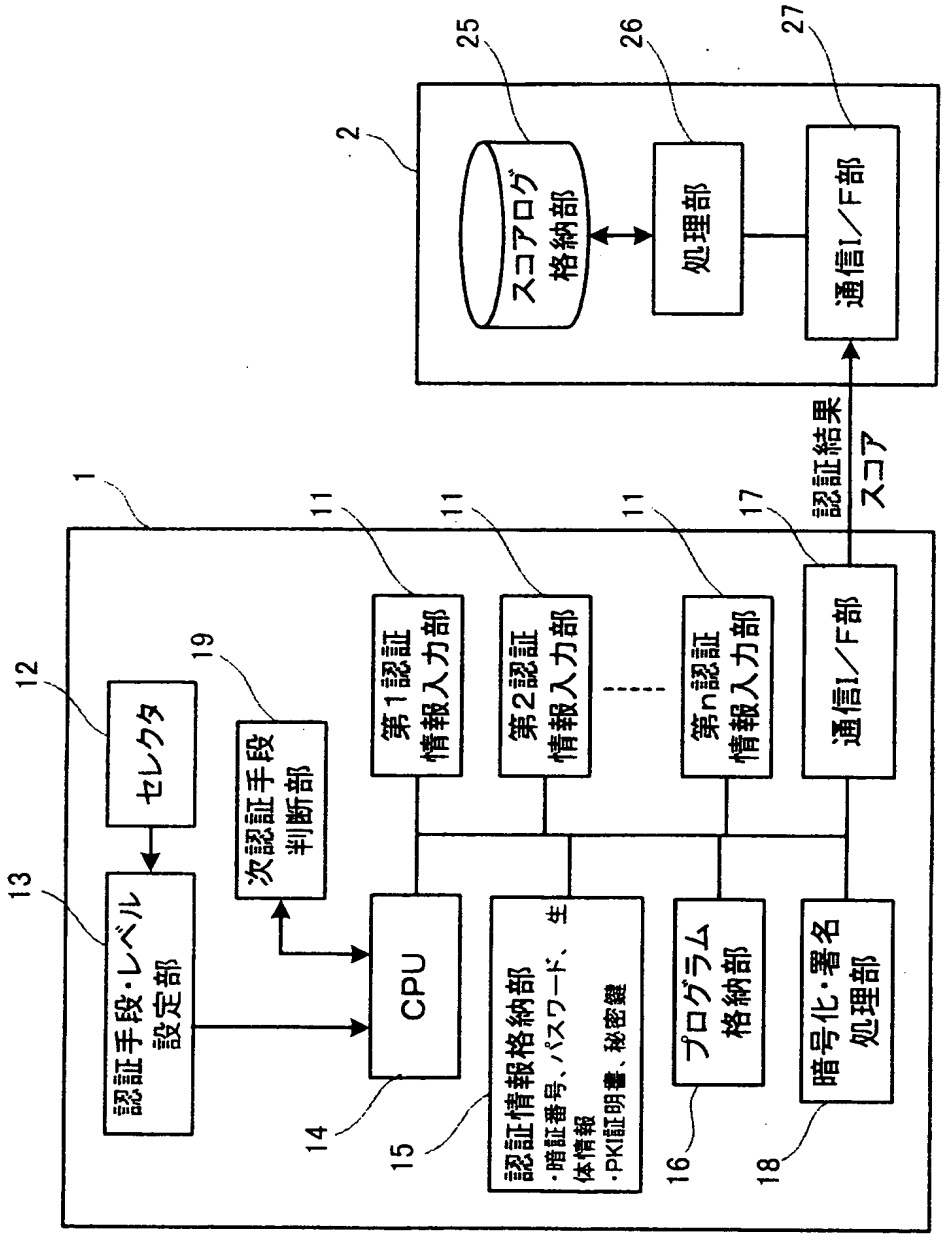
【図３】

個人認証端末をICカードとICカードリーダライタとの組合せによって構成した例を示すブロック図



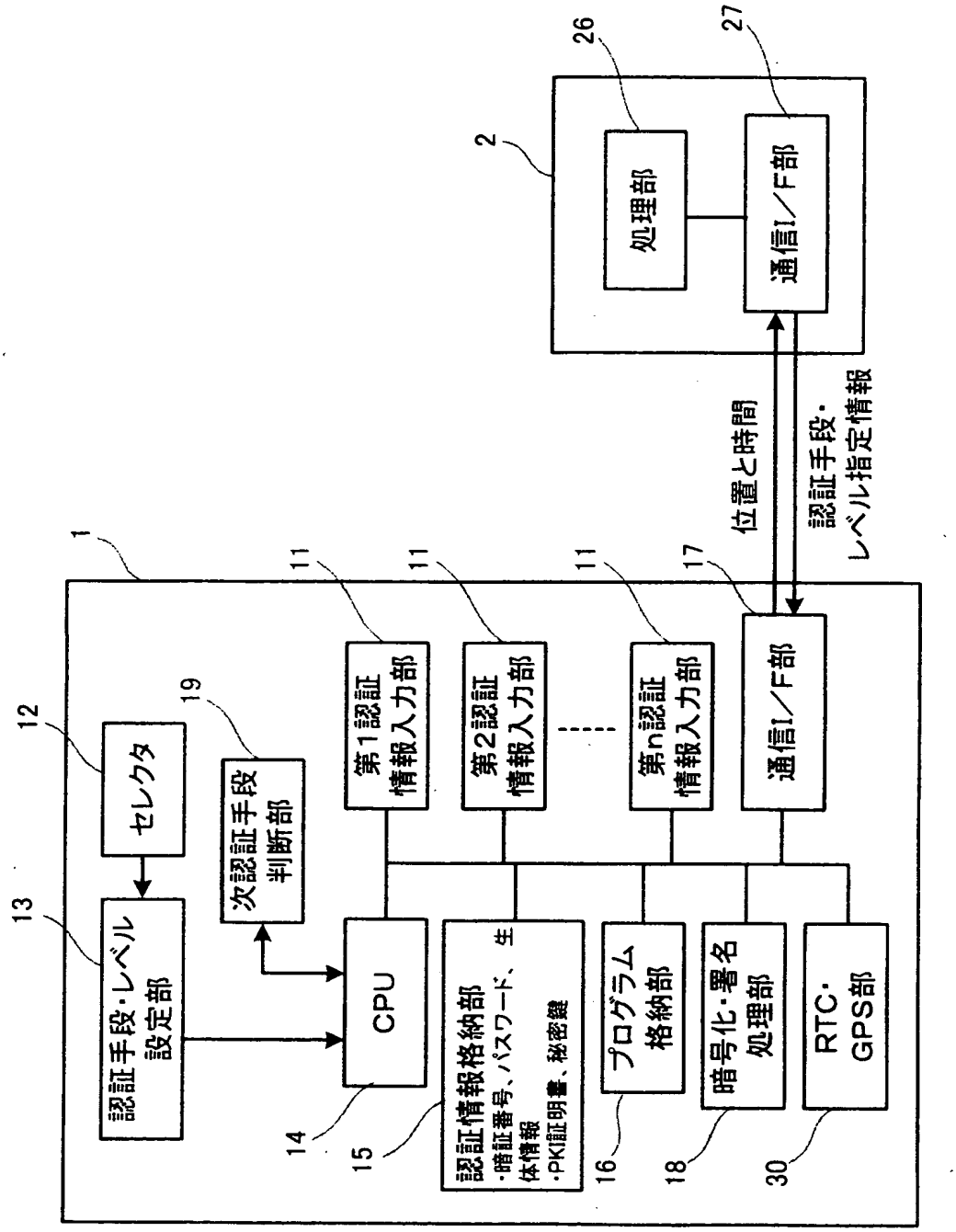
【図４】

一定の条件を満たした場合にサーバー側で認証不合格と判断するシステム構成の例を示すブロック図



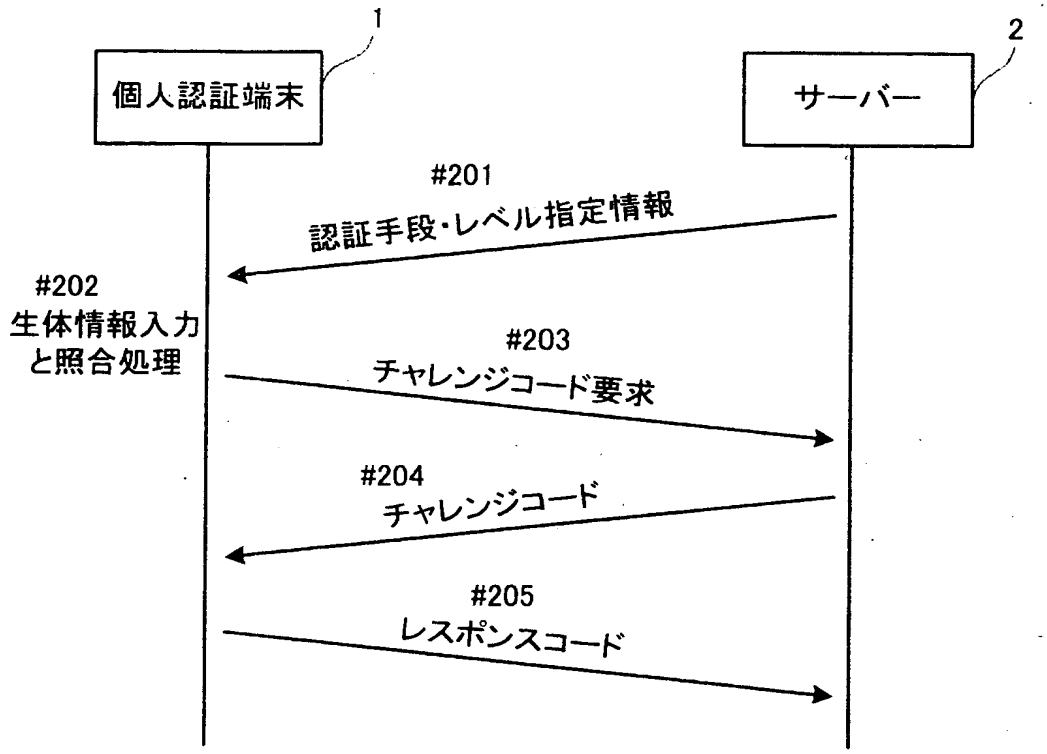
【図５】

個人認証端末から取得した情報に基づいてサーバーが認証手段･レベル指定情報を変更するシステム構成の例を示すブロック図



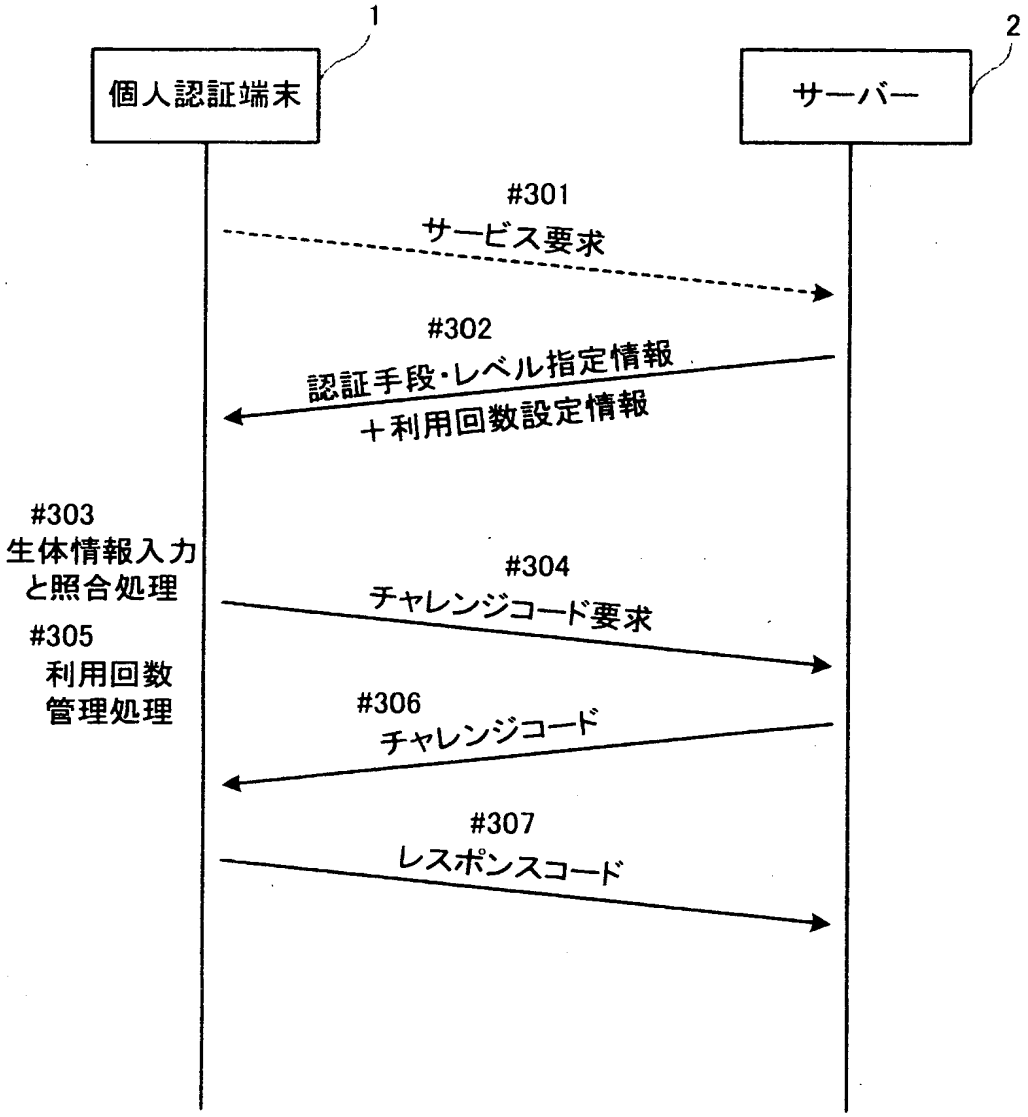
【図６】

チャレンジ＆レスポンスによる認証手段又は認証レベルの確認方法の例を示す図



【図７】

認証結果が合格である場合に、ユーザによる秘密鍵の利用回数を制限するための構成例を示す図



【書類名】　要約書

【要約】

【課題】　サーバーからの認証要求に応じて個人認証を実行する個人認証端末において、悪意のあるユーザによる不正使用を防止して認証結果の信頼性を高める。

【解決手段】　複数の認証手段又は認証レベルを備え、使用する認証手段又は認証レベルが可変である個人認証端末において、サーバー２から認証要求を受信するたびに、サーバー２から受信する認証手段・レベル指定情報にしたがって、使用する認証手段又は認証レベルを設定する。また、実際の認証に使用した認証手段又は認証レベルを特定する使用手段・レベル情報を認証結果と共に改竄検出可能な形式でサーバーに返す。

【選択図】　図１

特願２００２－３４５８５２

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　　神奈川県川崎市中原区上小田中１０１５番地
氏　名　　富士通株式会社

２．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社